APPLICATION FOR

UNITED STATES LETTERS PATENT

FOR

ELECTRONIC NOTARY SERVICE

BY:

Robert Rice
Jason Streit

Certificate under 37 CFR 1.10 of Mailing by "Express Mail"

EV 333420658 US
"Express Mail" label number

February 23, 2004
Date of Deposit

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Signature of person mailing correspondence

Cynthia Brock
Typed or printed name of person mailing correspondence

ELECTRONIC NOTARY SERVICE

BACKGROUND OF THE INVENTION

1. Technical Field:

The present invention relates to electronic document processing and more specifically to a method for collecting, verifying, and notarizing documents through a decentralized system, while satisfying federal and local legal formalities.

2. Description of Related Art:

Many legal documents require notarization to verify their authenticity. While the general concept of notarization crosses legal jurisdictions, each jurisdiction has its own unique, local requirements for proper notarization. These local requirements include qualifications to become a notary as well as formalities regarding the proper language, seal or stamp used for the notarization.

A problem often encountered with notarization of legal documents is geographic distance between parties to a document. In such a scenario, the documents must be physically sent to one party, who signs them and has them notarized by a local notary in accordance with local legal requirements. The documents are then usually returned to the sending party (i.e. attorney), who then send the documents to a second party, who similarly has them properly notarized, etc. Needless to say, this process is cumbersome and time consuming and also runs the risk of losing documents while sending them back and forth.

Therefore, it would be desirable to have a method and system for collecting properly notarized documents electronically through a geographically decentralized network of notaries.

SUMMARY OF THE INVENTION

The present invention provides a method, program, and system for notarizing and verifying documents via a distributed computer network. The invention includes creating an electronic version of the document on a client computer in the network, which is then encrypted and stored on a secure server in the computer network, wherein the stored electronic document may be retrieved by any client in the computer network. The signing party is then notified of the electronic document's identity and directed to the location of a certified notary within the signing party's geographic vicinity. The signing party visits the notary and retrieves the electronic document on the notary's client computer. The signing party then electronically signs the document using an electronic writing pad. The notary verifies the transaction and affixes his electronic signature to the document and also affixes an electronic image of his notary seal to the document and saves it on the server. Any certified notary in the network may then retrieve the signed, notarized document.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, however, as well as a preferred mode of use, further objectives and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 is a pictorial representation of a network of data processing systems in which the present invention may be implemented;

Figure 2, a block diagram of a data processing system that may be implemented as a server is depicted in accordance with a preferred embodiment of the present invention;

Figure 3 is a block diagram illustrating a data processing system in which the present invention may be implemented;

Figure 4 is a flowchart illustrating the process of notarizing a document electronically in accordance with the present invention;

Figure 5 is a flowchart illustrating an alternate notarization process in which a non-client individual wants to send a document for signing that requires notarization or verification;

Figure 6 is a flowchart illustrating in more detail the login process of accessing the Notary Service;

Figure 7 is a flowchart illustrating in more detail the process of adding a signature coordinate to a document;

Figure 8 is a flowchart illustrating the process of moving an existing coordinate in a document; and

Figure 9 is a flowchart illustrating the process of resizing an existing coordinate.

DETAILED DESCRIPTION OF THE INVENTION

With reference now to the figures, **Figure 1** is a pictorial representation of a network of data processing systems in which the present invention may be implemented. Network data processing system **100** is a network of computers in which the present invention may be implemented. Network data processing system **100** contains a network **102**, which is the medium used to provide communications links between various devices and computers connected together within network data processing system **100**. Network **102** may include connections, such as wire, wireless communication links, or fiber optic cables.

In the depicted example, a server **104** is connected to network **102** along with storage unit **106**. In addition, clients **108**, **110**, and **112** also are connected to network **102**. These clients **108**, **110**, and **112** may be, for example, personal computers or network computers. In the depicted example, server **104** provides data, such as boot files, operating system images, and applications to clients **108-112**. Network data processing system **100** might also contain a supplementary server **126** and additional data storage **128**.

Clients **108**, **110**, and **112** are clients to server **104**. Network data processing system **100** includes printers **114**, **116**, and **118**, and may also include additional servers, clients, and other devices not shown. The means by which clients **108-112** connect to the network **102** may include conventional telephone landline **120**, broadband Digital Service Line (DSL) or cable **124**, or wireless communication network **122**.

In the depicted example, network data processing system **100** is the Internet with network **102** representing a worldwide collection of networks and gateways that use the TCP/IP suite or similar protocols to communicate with one another. At the heart of the Internet is a backbone of high-speed data communication lines between major nodes or host computers, consisting of thousands of commercial, government, educational and other computer systems that route data and messages. Of course, network data processing system **100** also may be implemented as a number of different types of networks, such as for example, an intranet, a local area network (LAN), or a wide area network (WAN). **Figure 1** is intended as an example, and not as an architectural limitation for the present invention.

Referring to **Figure 2**, a block diagram of a data processing system that may be implemented as a server, such as server **104** in **Figure 1**, is depicted in accordance with a

preferred embodiment of the present invention. Data processing system **200** may be a symmetric multiprocessor (SMP) system including a plurality of processors **202** and **204** connected to system bus **206**. Alternatively, a single processor system may be employed. Also connected to system bus **206** is memory controller/cache **208**, which provides an interface to local memory **209**. I/O bus bridge **210** is connected to system bus **206** and provides an interface to I/O bus **212**. Memory controller/cache **208** and I/O bus bridge **210** may be integrated as depicted.

Peripheral component interconnect (PCI) bus bridge **214** connected to I/O bus **212** provides an interface to PCI local bus **216**. A number of modems may be connected to PCI bus **216**. Typical PCI bus implementations will support four PCI expansion slots or add-in connectors. Communication links to network computers **108-112** in **Figure 1** may be provided through modem **218** and network adapter **220** connected to PCI local bus **216** through add-in boards.

Additional PCI bus bridges **222** and **224** provide interfaces for additional PCI buses **226** and **228**, from which additional modems or network adapters may be supported. In this manner, data processing system **200** allows connections to multiple network computers. A memory-mapped graphics adapter **230** and hard disk **232** may also be connected to I/O bus **212** as depicted, either directly or indirectly.

Those of ordinary skill in the art will appreciate that the hardware depicted in **Figure 2** may vary. For example, other peripheral devices, such as optical disk drives and the like, also may be used in addition to or in place of the hardware depicted. The depicted example is not meant to imply architectural limitations with respect to the present invention.

The data processing system depicted in **Figure 2** may be, for example, an eServer pSeries system, a product of International Business Machines Corporation in Armonk, New York, running the Advanced Interactive Executive (AIX) or Linux operating systems.

With reference now to **Figure 3**, a block diagram illustrating a data processing system is depicted in which the present invention may be implemented. Data processing system **300** is an example of a client computer. Data processing system **300** employs a peripheral component interconnect (PCI) local bus architecture. Although the depicted example employs a PCI bus, other bus architectures such as Accelerated Graphics Port (AGP) and Industry Standard Architecture (ISA) may be used. Processor **302** and main memory **304** are connected to PCI local bus **306** through PCI bridge **308**. PCI bridge **308** also may include an integrated memory

controller and cache memory for processor **302**. Additional connections to PCI local bus **306** may be made through direct component interconnection or through add-in boards. In the depicted example, local area network (LAN) adapter **310**, SCSI host bus adapter **312**, and expansion bus interface **314** are connected to PCI local bus **306** by direct component connection. In contrast, audio adapter **316**, graphics adapter **318**, and audio/video adapter **319** are connected to PCI local bus **306** by add-in boards inserted into expansion slots. Expansion bus interface **314** provides a connection for a keyboard and mouse adapter **320**, modem **322**, and additional memory **324**. An electronic signature pad **326** and or biometric device or other authorization device is connected to the client computer **300** by common input interface.

Small computer system interface (SCSI) host bus adapter **312** provides a connection for hard disk drive **326**, tape drive **328**, and CD/DVD-ROM drive **330**. Typical PCI local bus implementations will support three or four PCI expansion slots or add-in connectors.

An operating system runs on processor **302** and is used to coordinate and provide control of various components within data processing system **300** in **Figure 3**. The operating system may be a commercially available operating system, such as Windows 2000, which is available from Microsoft Corporation. An object oriented programming system such as Java may run in conjunction with the operating system and provide calls to the operating system from Java programs or applications executing on data processing system **300**. "Java" is a trademark of Sun Microsystems, Inc. Instructions for the operating system, the object-oriented operating system, and applications or programs are located on storage devices, such as hard disk drive **326**, and may be loaded into main memory **304** for execution by processor **302.**

Those of ordinary skill in the art will appreciate that the hardware in **Figure 3** may vary depending on the implementation. Other internal hardware or peripheral devices, such as flash ROM (or equivalent nonvolatile memory) or optical disk drives and the like, may be used in addition to or in place of the hardware depicted in **Figure 3**. Also, the processes of the present invention may be applied to a multiprocessor data processing system.

As another example, data processing system **300** may be a stand-alone system configured to be bootable without relying on some type of network communication interface, whether or not data processing system **300** comprises some type of network communication interface. As a further example, data processing system **300** may be a Personal Digital Assistant (PDA) device,

which is configured with ROM and/or flash ROM in order to provide non-volatile memory for storing operating system files and/or user-generated data.

The depicted example in **Figure 3** and the above-described examples are not meant to imply architectural limitations. For example, data processing system **300** also may be a notebook computer or hand-held computer in addition to taking the form of a PDA. Data processing system **300** also may be a kiosk or a Web appliance.

Referring to **Figure 4**, a flowchart illustrating the process of notarizing a document electronically is depicted in accordance with the present invention. This process applies to professional clients of the Notary Service that routinely create legal documents requiring notarization and verification. Examples of such clients include law firms, title companies, banks, insurance companies, real estate companies, and justices of the peace.

The process begins when a Certified Creator (CC) creates a copy of a legal document within any application running in a Windows environment, e.g., MS Word, MS Excel, or Word Perfect (step **401**). After the document is created, a Certified Notary (CN) or CC clicks to start the session and a Notary Application Creation Wizard enters the document into the Notary Application running on the CC's client computer, where it is converted and encrypted (step **402**). The Application then creates an acceptance option for the Consent to Electronic Records (CER) of the transaction (step **403**). This acceptance option will be automatically saved and can be presented to the signer when the document is accessed for signature (described below).

The CC clicks on the Creation Wizard and enters the sender's information (step **404**) and the signer's information into the document (step **405**). The CC then determines the coordinates within the document that are designated for the signature or initials of the customer signer, as well as for a notary's signature, seal, dates, and time (step **406**). Steps **405** and **406** can be repeated for additional signers to the document. The Notary Application assigns a unique document number and the CC issues a unique password for the document in question and prints an invoice for the customer. (step **407**). The creation of the document is now complete, and the document is saved in a database on a server that can be accessed by any Certified Notary (CN) in the network (step **408**).

The CC notifies the customer signer of the document number and password, as well as the location and contact information for the nearest CN in the signer's area (step **409**).

The customer signer visits the CN in his or her area and provides the document number and password, which the CN uses to retrieve the document from the central database after the CN has been authenticated and logged into the application (step **410**). Once the document is pulled up and has been reviewed, and the Signing Customer or, the CN clicks a "sign" button (step **411**), the Sign Wizard starts and the customer signer must decide whether to accept or reject the CER (Step **412**).

If the signer rejects the CER, the Notary Application quits. If the signer accepts the CER, Notification is saved and the process continues, and the CN selects the signer's name from a list and enters any missing information (step **413**). The signer reviews and signs the document electronically (step **414**). The signature can be obtained using an electronic signature pad, similar to those used in retail credit card transactions. The CN then gathers verification information and document type and enters this information into the Notary Application (step **415**).

The CN verifies and documents the transaction, i.e. identity of the customer signer, document type, type of notarization, acknowledgement, Jurat, oath, etc. (step **416**) and signs the document and affixes the official notary seal, which is stored electronically by the Notary Application (step **417**). The notary signature may either be added using an electronic signature pad or stored in the Notary Application on the CN's client. The Notary Application automatically enters the date and time of the transaction into designated coordinates. The CN saves the document and can print a copy of the document for the customer signer (step **418**). The Application can also print an invoice.

An electronic notification (i.e. email) is sent back to the sender confirming that the document has been signed by the customer signer in question and properly notarized by the local CN (step **419**). The document can then be retrieved by the sender CC or another CN should additional signatures be necessary. An electronic notary journal or register file is automatically generated and updated containing all the necessary information regarding the transaction (step **420**). The journal may include information about the sender, sending customer, time, dates, type of document, fees, type of notarization, and signer's signature and verification information. All of this information is saved to the specific notary's journal database with in the notary application. The notary can then recall the journal within the Notary Application at any time.

The notary network described above may also have differing levels of access for Certified Creators and Certified Notaries. For example, Certified Notaries (including consulates, court clerks, or anyone with legal authority to verify/notarize a document) may be allowed to both create and verify/notarize documents. However, Certified Creators (e.g., secretaries, paralegals, bank officers, etc.) may be allowed to create documents but have no authority to verify/notarize the documents.

Figure 5 is a flowchart illustrating an alternate notarization process in which a non-client individual wants to send a document for signing that requires notarization or verification. This process applies to individuals who occasionally need to send documents for signature and notarized and would access the Notary Service via walk-in service providers and retailers, e.g., copy centers, hotel business offices, package stores, banks, etc.

The process begins with the sending customer creating the document in a standard computer application, e.g., Word Perfect, MS Word, Excel, etc., and saves it to disk (step **501**). The sending customer then visits the Notary Service web site and finds a CN in his area (step **502**).

The Sending customer visits the CN and presents the disk containing the document, and the CN starts the session on the Notary Application (step **503**). The CN opens a Create "wizard" to create a version of the document in the Notary Application (step **504**). The sending customer then chooses to accept or reject the CER (step **505**). If the customer rejects the acceptance, the session ends and the application quits.

If the customer accepts the CER, the process continues and CN enters the customer's personal information into the Notary Application (step **506**) and the signing party's information (step **507**) and then draws the signature coordinates for the signing party and notary (step **508**). The Application assigns a document number and the CC or CN enters a unique password (which is provided to the sending customer) and prints the document and presents an invoice. (step **509**). The document is now created and saved in the Notary Service database on a server and may be accessed by a CN in the network (step **510**).

At this point the sending customer can notify the signing customer about the document and provide the document number and password (step **511**). The location of a local CN in the signing party's area can be obtained from the Notary Service web site by either the sending customer or signing party (step **512**).

Similar to the process in **Figure 4**, the signing customer visits a local CN and retrieves the document from the database using the document number and password (step **513**). Once the document is pulled up, the CN clicks a "sign" button (step **514**), and the signing customer has to accept or reject the CER (Step **515**).

The CN selects the signer's name from a list and enters any missing information (step **516**). The signing customer signs the document using an electronic signature pad as described above (step **517**). The CN verifies and documents the transaction, i.e. identity of the customer signer, document type, type of notarization, acknowledgement, Jurat, oath, etc. (step **518**) and signs the document and affixes the proper seal (step **519**). The CN saves the document and prints a copy of the document for the signing customer (step **520**) application prints an invoice for the customer signer. The sending customer may then retrieve the signed, notarized document at any CN or CC location (step **521**). After the transaction is complete, a notary journal is updated, as explained above (step **522**).

Figure 6 is a flowchart illustrating in more detail the login process of accessing the Notary Service. The user begins by clicking on the Login button from either the File menu or a toolbar (step **601**). In response, the Notary Application displays the Login dialog box (step **602**). The user enters his or her name and password and clicks the Login button in the dialog box (step **603**), and the Application determines if the credentials entered by the user are valid (step **604**). If the credentials are invalid, the dialog box displays and error message (step **605**). If the user's credentials are valid, the Notary Application enables the menu and toolbar (step **606**).

Figure 7 is a flowchart illustrating in more detail the process of adding a signature coordinate to a document. The user navigates to the appropriate page in the document on which the signers are to affixes their signatures (step **701**). The user presses and holds down the left mouse button (step **702**), drags the mouse until the box is the appropriate size to accommodate the signature (step **703**) and releases the left mouse button (step **704**). The user then selects for who the coordinate is intended (i.e. signing customer or notary) and for what type of information the coordinate is intended (i.e. signature, date, or notary seal) (step **705**).

Figure 8 is a flowchart illustrating the process of moving an existing coordinate in a document. The user begins by clicking anywhere inside an existing coordinate, which highlights the boundary of the coordinate (step **801**). While holding down the left mouse button, the user

drags the coordinate to a new location (step **802**), and then releases the left mouse button, fixing the coordinate in its new location (step **803**).

Referring to **Figure 9**, a flowchart illustrates the process of resizing an existing coordinate. The user begins by clicking anywhere inside the existing coordinate, which highlights the boundary of the coordinate (step **901**). The user then clicks on one of the "grab handles" along the boundary of the coordinate (step **902**). While holding down the left mouse button, the user drags the grab handle until the coordinate is the desired size (step **903**) and then releases the left mouse button (step **904**).

As stated above, the present invention can be implemented with different user classes with specific abilities, duties, and restrictions. These user types may include notaries, document creators, county clerks, state certification agents, etc. Examples of legal document to which the present invention may apply include contracts, affidavits, Apostilles, foreign consulate documentation, wills, codicils, etc. Users can be any certified or commissioned user that has domestic or foreign authority by law to verify or authenticate the signer of a document.

The description of the present invention has been presented for purposes of illustration and description, and is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art. The embodiment was chosen and described in order to best explain the principles of the invention, the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.